

## REMARKS

Applicants request favorable reconsideration and allowance of the present application in view of the foregoing amendments and the following remarks.

Claims 38-42, 45-50, 53-58, 61-66, and 69-73 are pending in the present application. Claims 38-41 are the independent claims.

Claims 38-41 have been amended. Applicants submit that support for these amendments can be found in the original disclosure at least, for example, at page 12, lines 5-7 of the specification. Therefore, no new matter has been added.

Claims 38, 39, 40, 41, 42, 45-47, 50, 53-55, 58, 61-63, 66, 69-70, and 73 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,611,599 (Natarajan). Claims 48, 49, 56, 57, 64, 65, 71, and 72 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Natarajan. Applicants respectfully traverse these rejections for the reasons discussed below.

As discussed in the background section of the specification (e.g., page 2, line 2 through page 3, line 7), one conventional system for checking whether digital data has been altered involves applying a hash function to the digital data and then using a private key to encrypt the result of the hash function to obtain a digital signature. The digital signature is transmitted together with the digital data to a receiving device. At the receiving device, the digital signature is decrypted using a public key corresponding to the private key, and the same hash function that was used at the transmitting side is applied to the received digital data. The result of applying the hash function to the received digital data is compared to the decrypted digital signature and, if there is a match, then the digital data has not been altered.

In summary, this conventional system first applies a hash function (i.e., a one-way function) to digital data and then encrypts the result with a private key. A drawback of this system is that the private key/public key encryption requires a lot of processing power, and it is therefore difficult to make a system that is both fast (i.e., has the needed processing power) and compact. (See, e.g., page 3, line 13 through page 4, line 1 of the specification.)

The present invention as recited in independent Claim 38 addresses this problem. In particular, the invention as recited in independent Claim 38 includes, *inter alia*, the features of performing a predetermined calculation using an encoded digital image and confidential information and generating additional data by applying a one-way function to a result of the predetermined calculation. In other words, a predetermined calculation that uses both the encoded digital image and confidential information is first performed, and then a one-way function (e.g., a hash function) is applied to the result of the predetermined calculation. In this manner, a receiving device can check whether the digital image has been altered, but it is not necessary to perform private key/public key encryption and decryption. As a result, less processing power is needed and it is easier to make a device that is fast and compact.

Applicants submit that the cited art fails to disclose or suggest at least the above-mentioned features. In particular, Applicants submit that Natarajan fails to disclose or suggest at least the features of performing a predetermined calculation using an encoded digital image and confidential information, and then generating additional data by applying a one-way function to a result of the predetermined calculation. Instead, that patent discloses performing a one-way hash function on a digital object to obtain a message digest

M. (Col. 4, lines 27-30), and then encrypting the message digest M using a private key.

Col. 4, lines 62-65.

Thus, just like the conventional system discussed in the background of Applicants' specification, Natarajan first applies a hash function and then performs encryption on the result of the hash function. That patent does not disclose or suggest performing a predetermined calculation using the encoded digital image and confidential information, as recited in Claim 38. To the contrary, a one way hash function merely operates on the input data itself (see Col. 4, lines 31-34 of Natarajan) and does not use any other data in its calculation (see Col. 4, lines 49-52). The confidential information in Natarajan is used in a *subsequent* step, i.e., the encryption step performed *after* the hash function.

Further, Natarajan does not disclose or suggest generating additional data using a result of a predetermined calculation and a one-way function. Rather, that patent discloses that the one-way hash function is used in the first step, not on the result of a predetermined calculation.

The Examiner asserts that the one way hash function calculation unit of Natarajan corresponds to the claimed calculation unit and that the confidential information corresponds to the private key. Applicants respectfully disagree. As discussed above, a hash function merely operates on the data to be hashed and does not use any additional parameters/data in performing the hash calculation. Therefore, the hash function does not perform a calculation using digital image data and confidential information..

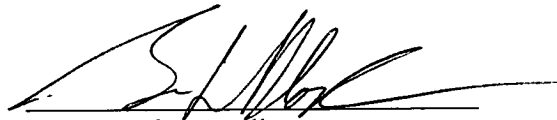
For the foregoing reasons, Applicants submit that the present invention recited in independent Claim 38 is patentable over the cited art. Independent Claims 39-41 recite features similar to Claim 38 and are believed patentable for similar reasons.

The dependent claims are believed patentable for at least the same reasons as the independent claims, as well as for the additional features they recite.

For the foregoing reasons, this application is believed to be in condition for allowance. Favorable reconsideration, withdrawal of the outstanding rejections, and an early Notice of Allowance are requested.

Applicants' undersigned attorney may be reached in our Washington, DC office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'B. L. Klock', written over a horizontal line.

Attorney for Applicants  
Brian L. Klock  
Registration No.36,570

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200  
BLK/lmj  
DC 171859v1